OIPE
AUG 24 2009
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of:	Confirmation No.: 7057
Bing WANG	Art Unit: 2456
Application No.: 10/748,459	Examiner: Kevin S. Mai
Filed: December 29, 2003	Attorney Dkt. No.: 059643.00747

For: METHOD AND SYSTEM FOR UNIFIED SESSION CONTROL OF MULTIPLE MANAGEMENT SERVERS ON NETWORK APPLIANCES

BRIEF ON APPEAL

August 24, 2009

I. INTRODUCTION

This is an appeal from the final rejection set forth in an Official Action dated December 8, 2008, finally rejecting claims 1-2 and 4-25. Claims 10 and 17 were objected to under 37 C.F.R. 1.75(c) as being improper dependent claims for failing to further limit the subject matter of their respective base claims. Claims 10 and 17 have been cancelled without prejudice or disclaimer and claim 11 has been amended to depend from claim 8 rather than claim 10. Claim 25 was rejected under 35 U.S.C. §101 because the claimed invention is allegedly directed to non-statutory subject matter. Claims 1-2 and 4-25 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2001/0047406 of Araujo *et al.* ("Araujo"). A Request for Reconsideration was timely filed on February 9, 2009.

08/25/2009 SMOHAMME 00000080 10748459
01 FC:1402 540.00 OP

An Advisory Action was mailed on April 8, 2009, indicating that the Request for Reconsideration had been considered, but did not place the application in condition for allowance. The Advisory Action also indicated that the claim amendments included in the Request for Reconsideration were to be entered for purposes of appeal. Therefore, claims 1-2, 4-9, 11-16, and 18-25 remain rejected.

A Notice of Appeal and a Pre-Appeal Brief Request for Review were timely filed on May 4, 2009. A Notice of Panel Decision from Pre-Appeal Brief Review was issued on July 24, 2009, indicating that the rejections of claims 1-2, 4-9, 11-16, and 18-25 were maintained. Accordingly, this Appeal Brief is being timely filed within one month of the Notice of Panel Decision.

II. REAL PARTY IN INTEREST

The real party in interest in this application is Nokia, Inc., of Irving, Texas, USA, by virtue of an Assignment by the inventor, which assignment was recorded at Reel 014860, Frame 0657, on December 29, 2003.

III. STATEMENT OF RELATED APPEALS AND INTERFERENCES

There are no known related appeals and/or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

IV. STATUS OF CLAIMS

Claims 1-2, 4-9, 11-16, and 18-25, all of the claims pending in the present application, are the subject of this appeal. Claims 1-2 and 4-25 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2001/0047406 of Araujo *et al.* ("Araujo"). Applicant filed a Response to the Office Action on February 9, 2009 ("Applicant's Response"). The Response cancelled claims 10 and 17 without prejudice or disclaimer and amended the dependency of claim 11. The Office issued an Advisory Action dated April 8, 2009 ("Advisory Action") indicating the cancellation of claims 10 and 17 and amendment of claim 11 had been entered for appellate purposes. Claim 25 was rejected under 35 U.S.C. §101 because the claimed invention is allegedly directed to non-statutory subject matter.

V. STATUS OF AMENDMENTS

A Notice of Appeal and a Pre-Appeal Brief Request for Review were filed on May 4, 2009. The amendments in the Response filed February 9, 2009, were entered for purposes of appeal. The claims are shown in the appropriate appendix to this brief as they were presented in the Response filed February 9, 2009, with the amendments to claim 11 shown as "Previously Presented" and the cancelled claims omitted, since they are no longer under appeal.

VI. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1, upon which claims 2 and 4-7 depend, is directed to a method. The method includes receiving (see, for example, Figure 4, box 402, page 10, lines 3-6) a request from a client device (see, for example, Client 102 in Figure 1, Network Appliance 214 in Figure 2, network appliance 314 in Figure 3, page 5, lines 15-17, page 6, lines 5-19, and page 8, lines 1-4) for access to an application associated with a network device (see, for example, Network Device 106 in Figure 1, page 5, lines 15-17, and page 6, lines 20-28). The method also includes establishing (see, for example, Figure 4, boxes 414 and 420, page 10, line 27, to page 11, line 22) a session between a unified session manager (see, for example, unified session manager 208 in Figure 2, unified session manager 308 in Figure 3, and page 8, lines 5-17) and a management server associated with the application (see, for example, management server 210 in Figure 2, management server 310 in Figure 3, and page 8, lines 1-25), wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device (see, for example, page 10, line 27, to page 11, line 22). The method further includes modifying the request at the unified session manager (see, for example, Figure 4, box 412, and page 10, lines 23-26). The method additionally includes forwarding, by the unified session manager, the modified request to the management server (see, for example, Figure 4, box 412, and page 10, lines 23-26). The method also includes receiving a response at the unified session manager from

the management server (see, for example, Figure 4, box 412, and page 10, lines 23-26). The method further includes modifying the response at the unified session manager (see, for example, Figure 4, box 412, and page 10, lines 23-26). The method additionally includes forwarding, by the unified session manager, the modified response to the client device (see, for example, Figure 4, box 412, and page 10, lines 23-26).

Independent claim 8, upon which claims 9 and 11-14 depend, is directed to an apparatus (see, for example, unified session manager 208 in Figure 2, unified session manager 308 in Figure 3, and page 8, lines 5-17). The apparatus includes a transceiver configured to receive (see, for example, Figure 4, box 402, page 10, lines 3-6) a request from a client (see, for example, Client 102 in Figure 1, Network Appliance 214 in Figure 2, network appliance 314 in Figure 3, page 5, lines 15-17, page 6, lines 5-19, and page 8, lines 1-4) for access to an application on the network device and to forward a response to the request. The apparatus also includes a processor, coupled to the transceiver, that is configured to establish (see, for example, Figure 4, boxes 414 and 420, page 10, line 27, to page 11, line 22) a session on behalf of the client between the unified session manager (see, for example, unified session manager 208 in Figure 2, unified session manager 308 in Figure 3, and page 8, lines 5-17) and a management server associated with the application (see, for example, management server 210 in Figure 2, management server 310 in Figure 3, and page 8, lines 1-25), wherein the session is established with the management server by the processor which is further configured to authenticate the unified session manager to

the management server, and wherein the authentication is virtually transparent to the client device (see, for example, page 10, line 27, to page 11, line 22), modify the request (see, for example, Figure 4, box 412, and page 10, lines 23-26), forward the modified request to the management server (see, for example, Figure 4, box 412, and page 10, lines 23-26), receive the response on behalf of the client from the management server associated with the application (see, for example, Figure 4, box 412, and page 10, lines 23-26), modify the response (see, for example, Figure 4, box 412, and page 10, lines 23-26), and forward the modified response from the management server to the transceiver (see, for example, Figure 4, box 412, and page 10, lines 23-26).

Independent claim 15, upon which claims 16 and 18 depend, is directed to a method. The method includes establishing (see, for example, Figure 4, boxes 414 and 420, page 10, line 27, to page 11, line 22) a session between a unified session manager (see, for example, unified session manager 208 in Figure 2, unified session manager 308 in Figure 3, and page 8, lines 5-17) and at least one of a plurality of the management servers (see, for example, management server 210 in Figure 2, management server 310 in Figure 3, and page 8, lines 1-25), wherein the unified session manager is enabled to operate on behalf of at least one of a plurality of clients (see, for example, Client 102 in Figure 1, Network Appliance 214 in Figure 2, network appliance 314 in Figure 3, page 5, lines 15-17, page 6, lines 5-19, and page 8, lines 1-4), and wherein establishing the session with the at least one of the management servers further comprises authenticating the unified session manager to the

management server, wherein the authentication is virtually transparent to the clients (see, for example, page 10, line 27, to page 11, line 22). The method also includes modifying (see, for example, Figure 4, box 412, and page 10, lines 23-26) each message from the at least one of the plurality of clients destined for an application associated with the at least one of the plurality of the managements servers, wherein the modification is virtually transparent to the client and to the management server (see, for example, page 10, line 27, to page 11, line 22).

Independent claim 19, upon which claims 20-22 depend, is directed to a method. The method includes retrieving a set of menu entries including at least one menu entry that is associated with a remote application (see, for example, page 3, lines 8-10). The method also includes displaying a selection menu on a display comprising the set of menu entries (see, for example, page 3, line 10). The method further includes retrieving a menu entry selection signal, wherein the menu entry selection signal is modified by a unified session manager (see, for example, page 3, lines 10-12). The method additionally includes forwarding (see, for example, page 3, lines 12-14) the modifying menu entry selection signal to a management server associated with the remote application (see, for example, management server 210 in Figure 2, management server 310 in Figure 3, and page 8, lines 1-25). The method also includes receiving another signal indicative of a response from the management server, wherein the other signal is modified by the unified session manager. The method further includes establishing (see, for example, Figure 4, boxes 414 and 420,

page 10, line 27, to page 11, line 22) a session between the unified session manager (see, for example, unified session manager 208 in Figure 2, unified session manager 308 in Figure 3, and page 8, lines 5-17) and the management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to a client device (see, for example, page 10, line 27, to page 11, line 22). The method additionally includes displaying the other modified signal at the display (see, for example, box 422 in Figure 4, and page 8, lines 19-22).

Independent claim 23 is directed to an apparatus (see, for example, unified session manager 208 in Figure 2, unified session manager 308 in Figure 3, and page 8, lines 5-17). The apparatus includes a means for establishing (see, for example, Figure 4, boxes 414 and 420, page 10, line 27, to page 11, line 22) a session with a management server associated with an application (see, for example, management server 210 in Figure 2, management server 310 in Figure 3, and page 8, lines 1-25) on behalf of a remote client (see, for example, Client 102 in Figure 1, Network Appliance 214 in Figure 2, network appliance 314 in Figure 3, page 5, lines 15-17, page 6, lines 5-19, and page 8, lines 1-4), wherein establishing the session with the management server further comprises authenticating means for authenticating the unified session manager (see, for example, unified session manager 208 in Figure 2, unified session manager 308 in Figure 3, and page 8, lines 5-17) to the management server, wherein the authenticating means is virtually transparent to the

client (see, for example, page 10, line 27, to page 11, line 22). The apparatus also includes a means of modifying a request (see, for example, Figure 4, box 412, and page 10, lines 23-26). The apparatus further includes a first forwarding component configured to forward the modified request to the management server (see, for example, Figure 4, box 412, and page 10, lines 23-26). The apparatus additionally includes a means for receiving a response from the management server (see, for example, Figure 4, box 412, and page 10, lines 23-26). The apparatus also includes a means for modifying the response (see, for example, Figure 4, box 412, and page 10, lines 23-26). The apparatus further includes a second forwarding component configured to forward the modified response to the remote client (see, for example, Figure 4, box 412, and page 10, lines 23-26).

Independent claim 24 is directed to an apparatus (see, for example, unified session manager 208 in Figure 2, unified session manager 308 in Figure 3, and page 8, lines 5-17). The apparatus includes an establisher configured to establish (see, for example, Figure 4, boxes 414 and 420, page 10, line 27, to page 11, line 22) a session with a management server associated with an application (see, for example, management server 210 in Figure 2, management server 310 in Figure 3, and page 8, lines 1-25) on behalf of a remote client (see, for example, Client 102 in Figure 1, Network Appliance 214 in Figure 2, network appliance 314 in Figure 3, page 5, lines 15-17, page 6, lines 5-19, and page 8, lines 1-4), wherein the session is established with the management server by an authentication with a unified session manager (see, for example, unified session manager 208 in Figure 2, unified

session manager 308 in Figure 3, and page 8, lines 5-17) to the management server, and wherein the authentication is virtually transparent to the remote client (see, for example, page 10, line 27, to page 11, line 22). The apparatus also includes a modifier configured to modify a request (see, for example, Figure 4, box 412, and page 10, lines 23-26). The apparatus further includes a request forwarder configured to forward the modified request to the management server (see, for example, Figure 4, box 412, and page 10, lines 23-26). The apparatus additionally includes a receiver configured to receive a response from the management server (see, for example, Figure 4, box 412, and page 10, lines 23-26). The apparatus also includes a modifier configured to modify the response (see, for example, Figure 4, box 412, and page 10, lines 23-26). The apparatus further includes a response forwarder configured to forward the modified response to the remote client (see, for example, Figure 4, box 412, and page 10, lines 23-26).

Independent claim 25 is directed to a computer program embodied on a computer readable medium, said computer program configured to control a processor (see, for example, unified session manager 208 in Figure 2, unified session manager 308 in Figure 3, and page 8, lines 5-17) to perform a process (see, for example, page 8, lines 18-21, and page 11, line 23, to page 12, line 2). The process includes receiving (see, for example, Figure 4, box 402, page 10, lines 3-6) a request from a client device (see, for example, Client 102 in Figure 1, Network Appliance 214 in Figure 2, network appliance 314 in Figure 3, page 5, lines 15-17, page 6, lines 5-19, and page 8, lines 1-4) for access to an

application associated with a network device (see, for example, Network Device 106 in Figure 1, page 5, lines 15-17, and page 6, lines 20-28). The process also includes establishing (see, for example, Figure 4, boxes 414 and 420, page 10, line 27, to page 11, line 22) a session between a unified session manager (see, for example, unified session manager 208 in Figure 2, unified session manager 308 in Figure 3, and page 8, lines 5-17) and a management server associated with the application (see, for example, management server 210 in Figure 2, management server 310 in Figure 3, and page 8, lines 1-25), wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device (see, for example, page 10, line 27, to page 11, line 22). The process further includes modifying the request at the unified session manager (see, for example, Figure 4, box 412, and page 10, lines 23-26). The process additionally includes forwarding, by the unified session manager, the modified request to the management server (see, for example, Figure 4, box 412, and page 10, lines 23-26). The process also includes receiving a response at the unified session manager from the management server (see, for example, Figure 4, box 412, and page 10, lines 23-26). The process further includes modifying the response at the unified session manager (see, for example, Figure 4, box 412, and page 10, lines 23-26). The process additionally includes forwarding, by the unified session manager, the modified response to the client device (see, for example, Figure 4, box 412, and page 10, lines 23-26).

VII. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed on appeal are the specific, detailed rejections of each of claims 1-2, 4-9, 11-16, and 18-25 under 35 U.S.C. §103(a) exactly as set forth in the Office Action of December 8, 2008, at pages 7-30. To summarize those grounds, claims 1-2 and 4-25 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2001/0047406 of Araujo *et al.* ("Araujo"). Applicant filed a Response to the Office Action on February 9, 2009 ("Applicant's Response"). The Response cancelled claims 10 and 17. The Office issued an Advisory Action dated April 8, 2009 ("Advisory Action") indicating the cancellation of claims 10 and 17 had been entered for appellate purposes. Claim 25 was rejected under 35 U.S.C. §101 because the claimed invention is allegedly directed to non-statutory subject matter.

VIII. APPELLANTS' ARGUMENTS

Appellant respectfully submits that each of pending claims 1-2, 4-9, 11-16, and 18-25 recites subject matter that is not taught, disclosed, or suggested by the cited art. Each of the claims is being argued separately under a separate sub-heading as suggested by 37 CFR 41.37(c)(1)(vii), and thus each of the claims stands or falls alone.

A. Rejection of claim 25

Claim 25 was rejected under 35 U.S.C. §101 because the claimed invention is allegedly directed to non-statutory subject matter. The Examiner alleged that the specification defines "computer-readable medium" in such a way that it "could include signals" and, thus, the claimed subject matter is non-statutory. Appellant respectfully traverses this rejection.

The Office Action has not identified any place where the term "computer-readable medium" is defined in such a way as to include signals. Quite to the contrary, the specification provides at page 5, line 18, and following several examples of computer readable media without ever once identifying a signal as such a medium. A computer readable medium is recognized as patentable subject matter under §101 and U.S. patent practice. Support for the definition of a computer readable medium is provided by *In re Lowry*, 32 F.3d 1579, 1583-1854, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994), which states: "When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in

most cases since use of technology permits the function of the descriptive material to be realized" (see §2106.01 of the MPEP). Thus, under U.S. precedent and the MPEP, the claims recite statutory subject matter.

A. Rejection of claims 1-2, 4-9, 11-16, and 18-25

Claims 1-2 and 4-25 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2001/0047406 of Araujo *et al.* ("Araujo"). Appellant respectfully traverses this rejection as applied to claims 1-2, 4-9, 11-16, and 18-25, claims 10 and 17 having been cancelled without prejudice or disclaimer.

In rejecting claims under 35 U.S.C. § 103, the Examiner bears the initial burden of presenting a *prima facie* case of obviousness. *See In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993). A *prima facie* case of obviousness is established by presenting evidence that the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the references before him to make the proposed combination or other modification. *See In re Lintner*, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972); *In re Vaeck*, 947 F.2d 488, 493, 20 USPQ2d 1438, 1442-43 (Fed. Cir. 1991) (explaining the three elements of a *prima facie* case of obviousness include: (1) motivation for the combination, (2) a reasonable expectation of success, and (3) a disclosure of all the claim elements by the prior art). *See also In re Royka*, 490 F.2d 981, 985, 180 USPQ 580, 583 (CCPA 1974).

Furthermore, the conclusion that the claimed subject matter is *prima facie* obvious

must be supported by evidence, as shown by some objective teaching in the prior art or by knowledge generally available to one of ordinary skill in the art that would have led that individual to combine the relevant teachings of the references to arrive at the claimed invention. *See In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

Rejections based on 35 USC § 103 must rest on a factual basis with these facts being interpreted without hindsight reconstruction of the invention from the prior art. The Examiner may not, because of doubt that the invention is patentable, resort to speculation, unfounded assumption, or hindsight reconstruction to supply deficiencies in the factual basis for the rejection. *See In re Warner*, 379 F.2d 1011, 1017, 154 USPQ 173, 178 (CCPA 1967). The Federal Circuit has repeatedly cautioned against employing hindsight by using Appellants' disclosure as a blueprint to reconstruct the claimed invention from the isolated teachings of the prior art. *See, e.g., Grain Processing Corp. v. American Maize-Prods. Co.*, 840 F.2d 902, 907, 5 USPQ2d 1788, 1792 (Fed. Cir. 1988).

When determining obviousness, "the [E]xaminer can satisfy the burden of showing obviousness of the combination 'only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references.'" *In re Lee*, 277 F.3d 1338, 1343, 61 USPQ2d 1430, 1434 (Fed. Cir. 2002), citing *In re Fritch*, 972 F.2d 1260, 1265, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992). "Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence.'" *In re Dembiczak*, 175

F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999). "Mere denials and conclusory statements, however, are not sufficient to establish a genuine issue of material fact." *Dembiczak*, 175 F.3d at 999-1000, 50 USPQ2d at 1617, *citing McElmurry v. Arkansas Power & Light Co.*, 995 F.2d 1576, 1578, 27 USPQ2d 1129, 1131 (Fed. Cir. 1993). Further, as pointed out by the Federal Circuit, the scope of the claim must be the first determination. "[T]he name of the game is the claim." *In re Hiniker Co.*, 150 F.3d 1362, 1369, 47 USPQ2d 1523, 1529 (Fed. Cir. 1998). It is respectfully submitted that the Office Action fails to meet the above-explained standard with respect to the rejections of any of the claims. Thus, it is respectfully requested that the rejections be reversed.

Araujo generally relates to an apparatus and accompanying methods for providing, through a centralized server site, an integrated virtual office environment, remotely accessible via a network-connected web browser, with remote network monitoring and management capabilities. In Araujo, a front end (a service enablement platform (SEP)) to one or more office servers on a LAN is connected to both the WAN and LAN and acts as a bridge between the user and the user's office applications. The front end also acts as a protocol translator to enable bi-directional, web-based, real-time communication to occur between the browser and each such application.

The Office Action has recognized that Araujo does not explicitly disclose that the feature of establishing a session between a unified session manager (SEP 200 of Araujo in the Office Action's view) and a management server associated with an application

comprises authenticating the unified session manager to the management server. However, the Office Action appears to have considered that this is implicit in Araujo, referring to paragraph [0109] of Araujo, which discloses that all information transfer for the Netilla virtual office is protected by SSL.

As such, the Office Action considered that the SEP and the application servers of Araujo communicate using SSL and that using SSL is known to inherently include an authentication step. Accordingly, the Office Action concluded that the SEP and the application servers authenticate themselves utilizing the SSL protocol in Araujo.

The Office Action's analysis is incorrect. While the Office Action is correct that the SSL protocol can include an authentication step, the Office Action is incorrect that the SEP and the application servers communicate using SSL in Araujo. Although Araujo does state in paragraph [0109] that for the Netilla virtual office, all information transfer is protected by SSL, if one reads further from this disclosure, it is made clear by Araujo that SSL encryption and decryption is only utilized for all communications **to and from the remote client via the WAN** and is not in fact used for communications **between the SEP and the LAN** including the application servers.

In paragraph [0109] of Araujo, it is explained that when an incoming packet is received at the SEP from the client device via the WAN connection, the open SSL module 304 performs SSL processing on the packet. This may implicitly involve authenticating the packet as suggested by the Office Action. It is then stated that after SSL processing, the

HTTP request is extracted and sent to the virtual office software 400 for translation into a form suitable for use by a desired office application. Once virtual office software 400 has properly processed the information, by providing suitable protocol conversion, that information flows **directly** from software 400 to the office application. Thus, it is clear that the incoming packet is authenticated and decrypted prior to extraction of the content of the packet extraction and subsequent translation by the virtual office software 400. The HTTP request is thus extracted, translated and sent directed to the office application without passing back via the open SSL module 340 for encryption prior to being sent to the application server. As such, there is no SSL encryption used for communications between the SEP and the application server.

The aforementioned interpretation (*i.e.* Appellant's interpretation) is confirmed as being correct with further reference to the disclosure in paragraph [0111] of Araujo, which describes the processing of packets received by the SEP from the LAN. These packets are received along data path 402 shown in Figure 3b. This path flows through to the virtual office software 400 without passing through web server 350 and without calling on the open SSL module 340. The virtual office software 400 generates an appropriate HTML page and only then passes the HTML page to web server 350. The web server 350 then calls on the services of the open SSL module 340 to encrypt the HTML page and send it to the remote client via the WAN.

In light of the above, it is clear that the mention of "all information transfer is

protected by SSL" in paragraph [0109] of Araujo actually relates to all information transferred **between the remote client and the SEP via the WAN**. No authentication and encryption protocols are utilized between the SEP and the LAN.

If there is any further doubt regarding the aforementioned analysis, Appellant respectfully further points out that the reason no encryption protocol is required in Araujo between the SEP and the LAN is that the SEP is authenticated during an initial installation process with the centralized administrative website (referred to as "customer care centre" (CCC)). This is described, for example, in paragraphs [0038] to [0041] of Araujo.

In light of the above, it is clear that there is no disclosure or suggestion in Araujo that establishing a session between the SEP and management server associated with an application comprises authenticating the SEP with the management server associated with the application. Rather, the SEP in Araujo is authenticated with a centralized administrative website (CCC) during installation and subsequent communications between a remote client and the SEP via the WAN are encrypted and decrypted using SSL.

The arrangement described in Araujo is adapted for use in small to medium sized organizations and specifically for remotely accessing an internal office network remotely by employees. A centralized administrative website (CCC) is used for remote network monitoring and management functionality. No authentication or encryption protocols are required between the SEP and the LAN as these are all located within the local office network environment. In contrast, certain embodiments of the present invention are

directed to a method and system for managing multiple management servers via a single unified session manager to provide a unified session control for general services over the internet to internet users who may not necessarily be employees looking to remotely access a local office network. As such, the applications and management servers associated therewith may not be provided in a safe office intranet environment. Accordingly, the arrangement of Araujo is not appropriate for the use intended for the present invention. For more general internet usage, it has been found by the present inventors to be advantageous that when a request is received from a client device for accessing an application, the step of establishing a session between a unified session manager and a management server associated with the application comprises authenticating the unified session manager to the management server. Such an authentication process is not required in Araujo.

It is noted that the Advisory Action argued that, despite the distinctions above, "this alone is not enough to determine that SSL would not be used between the SEP and the LAN." Appellant respectfully notes, however, that the burden is on the Office Action to positively demonstrate disclosure of the feature in the cited art, not on Appellant to prove non-disclosure. Accordingly, the appropriate standard is whether the disclosure is sufficient to positively establish disclosure of the claimed features. In this instance, it should be apparent that the disclosure in the art is not sufficient, as the art does not disclose the subject matter either explicitly, implicitly, or inherently.

1. Claim 1

In view of the arguments set forth above, it is respectfully submitted that "wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device" (as recited in claim 1), is neither disclosed nor suggested in Araujo. Thus, it is respectfully requested that the rejection of claim 1 be reversed

2. Claim 2

Claim 2 depends from and further limits claim 1. Thus, claim 2 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 1. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

3. Claim 4

Claim 4 depends from and further limits claim 1. Thus, claim 4 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 1. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

4. Claim 5

Claim 5 depends from and further limits claim 4. Thus, claim 5 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 4. This claim is being maintained separately to preserve Appellant's right to argue this

claim separately particularly in the event that a new ground of rejection is applied.

5. Claim 6

Claim 6 depends from and further limits claim 1. Thus, claim 6 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 1. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

6. Claim 7

Claim 7 depends from and further limits claim 1. Thus, claim 7 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 1. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

7. Claim 8

In view of the arguments set forth above, it is respectfully submitted that "establish a session on behalf of the client between the unified session manager and a management server associated with the application, wherein the session is established with the management server by the processor which is further configured to authenticate the unified session manager to the management server, and wherein the authentication is virtually transparent to the client device" (as recited in claim 8), is neither disclosed nor suggested in Araujo. Thus, it is respectfully requested that the rejection of claim 8 be reversed

8. Claim 9

Claim 9 depends from and further limits claim 8. Thus, claim 9 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 8. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

9. Claim 11

Claim 11 depends from and further limits claim 8. Thus, claim 11 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 8. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

10. Claim 12

Claim 12 depends from and further limits claim 8. Thus, claim 12 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 8. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

11. Claim 13

Claim 13 depends from and further limits claim 8. Thus, claim 13 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 8. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

12. Claim 14

Claim 14 depends from and further limits claim 8. Thus, claim 14 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 8. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

13. Claim 15

In view of the arguments set forth above, it is respectfully submitted that "establishing a session between a unified session manager and at least one of a plurality of the management servers, wherein the unified session manager is enabled to operate on behalf of at least one of a plurality of clients, and wherein establishing the session with the at least one of the management servers further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the clients" (as recited in claim 15), is neither disclosed nor suggested in Araujo. Thus, it is respectfully requested that the rejection of claim 15 be reversed

14. Claim 16

Claim 16 depends from and further limits claim 15. Thus, claim 16 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 15. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

15. Claim 18

Claim 18 depends from and further limits claim 15. Thus, claim 18 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 15. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

16. Claim 19

In view of the arguments set forth above, it is respectfully submitted that "establishing a session between the unified session manager and the management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to a client device" (as recited in claim 19), is neither disclosed nor suggested in Araujo. Thus, it is respectfully requested that the rejection of claim 19 be reversed

17. Claim 20

Claim 20 depends from and further limits claim 19. Thus, claim 20 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 19. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

18. Claim 21

Claim 21 depends from and further limits claim 19. Thus, claim 21 should be

allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 19. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

19. Claim 22

Claim 22 depends from and further limits claim 19. Thus, claim 22 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 19. This claim is being maintained separately to preserve Appellant's right to argue this claim separately particularly in the event that a new ground of rejection is applied.

20. Claim 23

In view of the arguments set forth above, it is respectfully submitted that "a means for establishing a session with a management server associated with an application on behalf of a remote client, wherein establishing the session with the management server further comprises authenticating means for authenticating the unified session manager to the management server, wherein the authenticating means is virtually transparent to the client" (as recited in claim 23), is neither disclosed nor suggested in Araujo. Thus, it is respectfully requested that the rejection of claim 23 be reversed

21. Claim 24

In view of the arguments set forth above, it is respectfully submitted that "an establisher configured to establish a session with a management server associated with an application on behalf of a remote client, wherein the session is established with the

management server by an authentication with a unified session manager to the management server, and wherein the authentication is virtually transparent to the remote client" (as recited in claim 24), is neither disclosed nor suggested in Araujo. Thus, it is respectfully requested that the rejection of claim 24 be reversed

22. Claim 25

In view of the arguments set forth above, it is respectfully submitted that "establishing a session between a unified session manager and a management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device" (as recited in claim 25), is neither disclosed nor suggested in Araujo. Thus, it is respectfully requested that the rejection of claim 25 be reversed

Conclusion

For all of the above noted reasons, it is strongly contended that certain clear differences exist between the present invention as claimed in claims 1-2, 4-9, 11-16, and 18-25, and the cited art relied upon by the Office Action. It is further contended that these differences are more than sufficient that the present invention would not have been obvious to a person having ordinary skill in the art at the time the invention was made. Additionally, each claim of the present application is directed to statutory subject matter.

This final rejection being in error, therefore, it is respectfully requested that this honorable Board of Patent Appeals and Interferences reverse the Examiner's decision in this case and indicate the allowability of application claims 1-2, 4-9, 11-16, and 18-25.

In the event that this paper is not being timely filed, the Appellant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees which may be due with respect to this paper may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,
SQUIRE, SANDERS & DEMPSEY LLP

Peter Flanagan
Attorney for Appellant
Registration No. 58,178

Atty. Docket No.: 059643.00747

8000 Towers Crescent Drive, 14th Floor
Vienna, VA 22182-6212
Tel: (703) 720-7800
Fax (703) 720-7802

PCF:dlh

Encls: Appendix 1 - Claims on Appeal
Appendix 2 - Evidence
Appendix 3 - Related Proceedings

APPENDIX 1

CLAIMS ON APPEAL

1. (Previously Presented) A method, comprising:

receiving a request from a client device for access to an application associated with a network device;

establishing a session between a unified session manager and a management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device;

modifying the request at the unified session manager;

forwarding, by the unified session manager, the modified request to the management server;

receiving a response at the unified session manager from the management server;

modifying the response at the unified session manager; and

forwarding, by the unified session manager, the modified response to the client device.

2. (Original) The method of Claim 1, wherein the request is authenticated by the unified session manager.

4. (Previously Presented) The method of Claim 1, wherein modifying the request further comprises translating a graphical user interface message and, wherein modifying the response further comprises translating another graphical user interface message.

5. (Previously Presented) The method of Claim 4, wherein at least one of the graphical user interface message and the other graphical user interface message is translated into a unified format.

6. (Original) The method of Claim 1, wherein modifying the request further comprises modifying a network address before forwarding the modified request, and wherein modifying the response further comprises modifying another network address before forwarding the modified response.

7. (Original) The method of Claim 1, wherein modifying the response further comprises enabling a download of a file from the unified session manager.

8. (Previously Presented) An apparatus, comprising:

a transceiver configured to receive a request from a client for access to an application on the network device and to forward a response to the request; and

a processor, coupled to the transceiver, that is configured to

establish a session on behalf of the client between the unified session manager and a management server associated with the application, wherein the session is established with the management server by the processor which is further configured to authenticate the unified session manager to the management server, and wherein the authentication is virtually transparent to the client device,

modify the request,

forward the modified request to the management server,

receive the response on behalf of the client from the management server associated with the application,

modify the response, and

forward the modified response from the management server to the transceiver.

9. (Previously Presented) The apparatus of Claim 8, wherein the processor is further configured to authenticate the request.

11. (Previously Presented) The apparatus of Claim 8, wherein the authentication to the management server further comprises sending at least one of a password, a certificate, and an encryption key.

12. (Previously Presented) The apparatus of Claim 8, wherein the processor is further configured to modify at least one of the request and the response by translating at least one graphical user interface message.

13. (Previously Presented) The apparatus of Claim 8 the processor is further configured to

establish another session on behalf of the client with another application,

modify another request,

forward the other modified request to the application,

receive another response on behalf of the client from the application,

modify the other response, and

forward the other modified response to the transceiver.

14. (Previously Presented) The apparatus of Claim 8, wherein the processor is further configured to enable a plurality of clients to access virtually simultaneously a plurality of applications on the network device.

15. (Previously Presented) A method, comprising:

establishing a session between a unified session manager and at least one of a plurality of the management servers, wherein the unified session manager is enabled to

operate on behalf of at least one of a plurality of clients, and wherein establishing the session with the at least one of the management servers further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the clients; and

modifying each message from the at least one of the plurality of clients destined for an application associated with the at least one of the plurality of the managements servers, wherein the modification is virtually transparent to the client and to the management server.

16. (Original) The method of Claim 15, wherein the unified session manager is enabled to operate on behalf of the plurality of clients seeking access to the at least one of the plurality of management servers.

18. (Previously Presented) The method of Claim 15, wherein modifying message between the at least one of the plurality of the clients and the at least one of the plurality of the management servers further comprises at least one of wrapping a Java applet, and translating a uniform resource locator.

19. (Previously Presented) A method, comprising:

retrieving a set of menu entries including at least one menu entry that is associated with a remote application;

displaying a selection menu on a display comprising the set of menu entries;

retrieving a menu entry selection signal, wherein the menu entry selection signal is modified by a unified session manager;

forwarding the modifying menu entry selection signal to a management server associated with the remote application;

receiving another signal indicative of a response from the management server, wherein the other signal is modified by the unified session manager;

establishing a session between the unified session manager and the management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to a client device; and

displaying the other modified signal at the display.

20. (Original) The method of Claim 19, wherein the menu entry selection signal comprises, a request for authentication, and a request for a program download.

21. (Previously Presented) The method of Claim 19, wherein modifying the menu entry selection signal further comprises translating a graphical user interface message, altering a network address, and attaching additional information to the signal.

22. (Previously Presented) The method of Claim 19, wherein modifying the other signal, indicative of a response from the management server, further comprises translating a graphical user interface message, altering a network address, and attaching additional information to the signal.

23. (Previously Presented) An apparatus, comprising:

a means for establishing a session with a management server associated with an application on behalf of a remote client, wherein establishing the session with the management server further comprises authenticating means for authenticating the unified session manager to the management server, wherein the authenticating means is virtually transparent to the client;

a means of modifying a request;

a first forwarding component configured to forward the modified request to the management server;

a means for receiving a response from the management server;

a means for modifying the response; and

a second forwarding component configured to forward the modified response to the remote client.

24. (Previously Presented) An apparatus, comprising:

an establisher configured to establish a session with a management server associated with an application on behalf of a remote client, wherein the session is established with the management server by an authentication with a unified session manager to the management server, and wherein the authentication is virtually transparent to the remote client;

a modifier configured to modify a request;

a request forwarder configured to forward the modified request to the management server;

a receiver configured to receive a response from the management server;

a modifier configured to modify the response; and

a response forwarder configured to forward the modified response to the remote client.

25. (Previously Presented) A computer program embodied on a computer readable medium, said computer program configured to control a processor to perform:

receiving a request from a client device for access to an application associated with a network device;

establishing a session between a unified session manager and a management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management

server, wherein the authentication is virtually transparent to the client device;

modifying the request at the unified session manager;

forwarding, by the unified session manager, the modified request to the management server;

receiving a response at the unified session manager from the management server;

modifying the response at the unified session manager; and

forwarding, by the unified session manager, the modified response to the client device.

APPENDIX 2

EVIDENCE APPENDIX

No evidence under section 37 C.F.R. 1.130, 1.131, or 1.132 has been entered or will be relied upon by Appellants in this appeal.

APPENDIX 3

RELATED PROCEEDINGS APPENDIX

No decisions of the Board or of any court have been identified under 37 C.F.R. §41.37(c)(1)(ii).